Radio Comms
WWW.RADIOCOMMS.COM.AU

Find

Radio Comms Asia-Pacific magazine

site index

- monthly newsletter
- subscribe to newsletter
- hot products
- feature articles

search + browse

- radiocomms directory
- RadioCommsCONNECT 2007

the magazine

- **FREE** subscription
- advertising info

online communities

- Telecomms/IT
- SearchNetworking
- SearchSecurity
- SearchStorage
- Electronics
- Laboratory
- Process Control
- InMotion
- Safety
- Food Processing
- Waste Technology
- BuynetPlus

12/2/2007

homepage advertising on this site about this s

previous

Is RFID s

Antenna i collaborat

Radio din with grow

article ar

archive 2(

archive 2(

archive 2(

archive 2(

feature articles

Is RFID safe and secure?

Elizabeth Latham, Radio Comms *journalist*

We've heard a lot about RFID - it's used in supermarkets, implanted in pets and even by blood banks - but is it actually secure? Is the information we put on these chips safe from hackers?

RFID is a very useful technology, especially in production because it is usually non-line-of-sight (nLOS). This means that cartons or pallets do not require a particular orientation for scanning, unlike bar codes. This aids in the automation of many tasks throughout the supply chain that have typically been labour intensive, such as checking and scanning incoming inventory.

Organisations also have an accurate picture of stock levels, which in turn means lower inventory costs and fewer out-of-stock occurrences.

Can you trust the RFID to hold your information?

Dr Katina Michael, senior lecturer in the School of Information Systems and Technology, Faculty of Informatics, University of Wollongong, believes it's all a matter of context, but would not advise the use of RFID for access control types of applications.

"Security has to be identified as the number one disadvantage of RFID. Although it should be stated that researchers are working hard to overcome this hurdle, offering a variety of partial solutions," Michael said.

While standards are beginning to emerge like EPCglobal, there is a great number of proprietary specific RFID standards on the market. The standard denotes how a message is stored, the length of a message (for example 128-bit) and a sequence of bits that tell a reader when to start and stop reading, as well as additional error-checking bits.

How does information get tampered with?

"It is as simple as acquiring the relevant reader and working out what each bit in the message means, and interpreting that information correctly. Bits can be encoded using a particular scheme, but once the scheme is identified, the information can be read," Michael said.

"Given RFID is wireless, you need be in the proximity of 90 centimetres (dependent on the range requirements of the tag) to intercept the radio signal. So once you have read the chip you can simply play back the signal you picked up and pretend to be someone you are not."

This has major implications for active tags because it means the hacker cannot only read information but write to the tag as well, and even change variables.

"When a new technology enters the market, hackers are presented with a new challenge. And so the race begins for who can 'crack the code' so to speak," Michael said.

How can you protect yourself from hackers?

There are many options to choose from when trying to protect data. For example, it is possible to kill off the RFID tag after a certain time and date-stamp on the chip. The information on the chip can also be encrypted and passwords placed on the tags.

Two main approaches have been adopted by researchers: either a separate piece of hardware is required (hard solution), or a software-based solution is adopted (soft solution). Blocker tags (such as ancillary RFID tags) can also help solve the problem of hacking by preventing unauthorised scanning of items.

It is also possible to use antennae energy analysis to gauge the distance of a reader from a tag or storing a biometric onboard the RFID chip.

"All the RFID security-privacy solutions being proposed are only partial solutions and each has its benefits and limitations. At the crux of the matter is the unique ID of the actual RFID tag, how this information is stored and whether or not passwords have a role to play and how anonymity is ensured," Michael said.

More recently, developments for human-centric applications have seen RFID go into the subdermal layer of the skin in the form of a transponder.

"The argument for this latest development to 'protect' information is simple - if it's beneath the skin the ID chip cannot be stolen, is with you everywhere you go, is lightweight, it cannot be duplicated, a perpetrator does not know you have something implanted, and the RFID chip can be accessed at crucial times with your prior consent," Michael said.

Michael warns that the benefits of the above method of protection are misleading. Chips can still be read by persons in close proximity to an implantee, or even by unobtrusive readers that can trigger the device to emit a signal.

So, you decide. Is the risk worth it? What information is on the RFID chip and do you want someone to have access to it?